Z Notation

ניר אדר

Z Notation

1. תוכן עניינים

2. פתיחה

שיטה פורמלית – דרך מדוייקת לתאר מה המערכת צריכה לבצע, מבלי לתאר כיצד המערכת תבצע זאת. בעזרת שיטות פורמליות אפשר לאתר תקלות בתכנון ולמנוע תקלות תכנות. אנחנו מתארים את התוכנית ומוכיחים את הנכונות שלה.

סכימת Z היא שיטה פורמלית לכתיבת מפרטים. היא פותחה באוניברסיטת אוקספורד בשנות ה-70.

מעט על מאפייני הסכימה:

- הסכימה מבוססת על פעולות בין קבוצות.
- אנו משתמשים בקבוצות עם הפעולות הרגילות – חיתוך, איחוד וכדו'.
- בנוסף – אנו נשתמש בסימונים נוספים מרחיבים את היכולת שלנו לבטא מערכות מורכבות.
- פעולות משפיעות על מצב המערכת.

מערכת מתוארת ע"י:

א. תיאור החלקים בתור מצב
ב. מצבים התחלתיים
ג. תיאור מה כל פעולה עושה למצב במערכת

נציג כעת את תורת הקבוצות, בכתיב בו משתמשים ב-Z. לאחר מכן נציג כיצד אנחנו משתמשים בצורת הקבוצות בסכימות של Z לייצוג מערכות.

3. קבוצות

3.1 הגדרת קבוצה

קבוצה היא אוסף של אובייקטים. ניתן לייצג קבוצה בדרכים שונות, אחת מהן היא למשל **ציון הפריטים בקבוצה**:

$$\{dog, cat, mouse\}$$

מתכונות הקבוצה:

- כל אובייקט מופיע בקבוצה פעם אחת.
- אין חשיבות לסדר בו הפרטים מופיעים. לדוגמא הקבוצה הבאה זהה לקבוצה הקודמת:

$$\{cat, dog, mouse\}$$

ייצוגים נוספים:

- **טווח מספרים**, למשל 1..7 – הינה הקבוצה המכילה את כל המספרים בין 1 ל-7 (כולל 1 ו-7).

3.2 קבוצות ידועות

- $\mathbb{Z}$ - קבוצת המספרים השלמים.
- $\mathbb{N}$ - קבוצת המספרים הטבעיים, כולל 0.
- $\mathbb{N}_1$ - קבוצת כל המספרים הטבעיים, לא כולל 0. $\left(\mathbb{N}/\{0\}\right)$
- $\varnothing$ - הקבוצה הריקה – קבוצה שאין בה איברים.

3.3 מושגים נוספים

- #S – **קרדינליות הקבוצה** – מספר האיברים בקבוצה סופית S. לא מוגדר עבור קבוצה אינסופית.
- **שוויון קבוצות** – 2 קבוצות A, B שוות אם יש להן את אותו מספר של איברים. נסמן $A = B$.

3.4. פעולות על מספרים

פעולות בין מספרים:

פעולה	פירוש
$m+n$	חיבור
$m-n$	חיסור
$m*n$	כפל
$m \operatorname{div} n$	חילוק
$m \bmod n$	מודולו
$succ\ n$	העוקב
$pred\ n$	הקודם

השוואה בין מספרים:

פעולה	פירוש
$m \leq n$	קטן או שווה
$m < n$	קטן
$m \geq n$	גדול או שווה
$m > n$	גדול
$m = n$	שוויון בין מספרים

פעולות על קבוצות מספרים:

פעולה	פירוש
$\min A$	האיבר המינימלי בקבוצה A
$\max A$	האיבר המקסימלי בקבוצה A

3.5. פעולות על קבוצות

- $A\bigcup B$ - איחוד קבוצות.
- $A\bigcap B$ - חיתוך קבוצות.
- $A\setminus B$ - הפרש בין קבוצות.
- $\bigcup A$ - איחוד כל תתי הקבוצות של A.
- $\bigcap A$ - חיתוך כל תתי הקבוצות של A.
- $first\ x$ - האיבר הראשון מבין זוג סדר.
- $second\ x$ - האיבר השני מבין זוג סדור.
- $\mathbb{P}(s)$ **קבוצת החזקה** של S – קבוצת כל תתי הקבוצות של S.
- $\mathbb{P}_1(s)$ קבוצת החזקה הלא ריקה של S.
- $\mathbb{F}(s)$ קבוצת כל תתי הקבוצות הסופיות של S

פעולות לוגיות:

- $\{x:T\mid p\}$קבוצת כל הפריטים מסוג T המספקים את p.
- $\forall x:T\bullet p$ - לכל x מסוג T מתקיים p
- $\{x:T\bullet f(x)\}$ קבוצת כל הפריטים מסוג T שהם $f(x)$.
- $\exists x:T\bullet p$ - קיים x מסוג T המקיים את הפרדיקט p.
- $\exists_1 x:T\bullet p$ - קיים בדיוק x אחד מסוג T המקיים את הפרדיקט p.

3.6. רלציות

3.6.1. הגדרות בסיסיות

תזכורת: **מכפלה קרטזית** $A\times B$ מוגדרת כך:

$$A\times B=\{\langle a,b\rangle \mid a\in A,b\in B\}$$

כלומר, קבוצת כל הקבוצות הסדורים שהאיבר הראשון בהם שייך ל-A והאיבר השני שייך ל-B.

רלציה היא תת קבוצה של $A\times B$. אוסף הרלציות האפשריות הוא היא קבוצת החזקה של $A\times B$.

כדי להגיד שהאיברים $a\in A$ ו-$b\in B$ נמצאים ברלציה נסמן aRb או $(a,b)\in R$.

תחום וטווח:

- **תחום:** $domR\equiv\{x:X \mid \exists y:Y.(x,y)\in R\}$
- **טווח:** $ranR\equiv\{y:Y \mid \exists x:X.(x,y)\in R\}$
- הערה: משמעות נקודותיים (":") היא "מסוג"

הרכבת רלציות:

יהיו רלציות R_1,R_2 נסמן **הרכבה** על ידי: ($R_1 \fatsemi R_2$)

פונקציות:

פונקציה היא רלציה עם "תוצאה" בודדת. כל פונקציה היא רלציה. לא כל רלציה היא פונקציה.

3.6.2. סוגי פונקציות

תזכורת:

- פונקציה $f : A \to B$ נקראת **חד חד ערכית** אם לכל $x, y \in A$ מתקיים: $x \neq y \Rightarrow f(x) \neq f(y)$.
- פונקציה $f : A \to B$ נקראת **על** אם לכל איבר $b \in B$ קיים $a \in A$ כך ש- $f(a) = b$.

צורת כתיבה	סוג פונקציה	הסבר
A⇸B	פונקציה חלקית	$dom(f) \subset A$ כל איבר ב-A מקשר לכל היותר לאיבר אחד ב-B.
A→B	פונקציה מלאה	$dom(f) = A$ כל איבר ב-A מקשר לאיבר אחד ב-B.
A⤔B	פונקציה חלקית חד חד ערכית	$dom(f) \subset A$ ובנוסף הפונקציה חד חד ערכית
A↣B	פונקציה מלאה חד חד ערכית	$dom(f) = A$ ובנוסף הפונקציה חד חד ערכית
A⤀B	פונקציה חלקית על	$dom(f) \subset A, ran(f) = B$
A↠B	פונקציה מלאה על	$dom(f) \subset A, ran(f) = B$

3.6.3. רלציות כקבוצות

דוגמא:

$$R_1=\{(A,1),(B,2)\} \qquad R_2=\{(C,3),(D,4)\}$$
$$R_1\cup R_2=\{(A,1),(B,2),(C,3),(D,4)\}$$
$$\#R_1=2$$

פונקציות ופעולות של קבוצות:

- **חיתוך של פונקציות** הוא פונקציה. (אבל במקרים רבים – הפונקציה הריקה $\varnothing$).
- **איחוד של פונקציות** אינו בהכרח פונקציה.
- **אופרטור חדש**: $f\oplus g$ - קבוצה המכילה את כל g ואת כל האלמנטים מ- f שלא יוצרים קונפליקט עם האיברים ב- g.
- **הפיכת רלציה לפונקציה:**

$$r:S\times T \qquad \{(A,1),(A,2)(B,3)\}$$

$$f:S\to \mathbb{P}T \qquad \{(A,\{1,2\}),(B,\{3\})\}$$

סימון נוסף לזוג "ממפה אל"

$$\{(1,A),(2,B)\}=\{1\mapsto A,2\mapsto B\}$$

הגבלות על תחום ועל טווח –

- S◁R – הגבלה על התחום של R על ידי S. לוקחים את החלק של R ש"מתחיל" ב-S:

S◁R=$\{a:A;b:B\mid a\in S\wedge a\mapsto b\in R\bullet a\mapsto b\}$

- R▷S – הגבלה על הטווח של הרלציה R על ידי S.
- קיימים שני אופרטורים מקבילים, בהם יש –, שפירושו "החלק שלא ב-S". האופרטורים הם ⩤⩥

סימונים נוספים:

$iter\, n\, R \equiv R^n \equiv R \cdot R \cdot R \cdot R ⨾ R \cdot R$

$R^{\sim}$ Inverse of relation $\left(R^{1}\right)$ $\{y : Y; x : X \mid xRy\}$

R^{*} $R^{*} \equiv \bigcup\{n : \mathbb{N} \bullet R^{n}\}$

R^{+} $R^{+} \equiv \bigcup\{n : \mathbb{N}^{+} \bullet R^{n}\}$

חוקים הישימים ל-dom:

$dom(f \cup g) = (dom\, f) \cup (dom\, g)$

$dom\{a \mapsto b\} = \{a\}$

4. סדרות – Sequences

4.1 הגדרה ומוטיבציה

לעתים אנחנו רוצים לממש אוסף סדור של איברים (**סידרה**). נממש אוסף כזה כך:

- תהיה X קבוצה (ולא סידרה).
- נגדיר פונקציה מהמספרים 1..N הממפה אל איברים ב-X. נסמן: seq[X]

כדי לזהות סדרה, נסמן את איבריה בסוגריים משולשים. דוגמא:

$$MySeq =< Moshe, David, Nir, Eyal >$$

סדרה ריקה תסומן כך: <>

הגדרה פורמלית: סדרה היא פונקציה שהתחום שלה הוא תת קבוצה רציפה $\{1..N\}$ של המספרים הטבעיים:

$$seq(A) \triangleq \{f:\mathbb{N} \cdot A \mid dom\ f = 1..\#f\}$$

4.2 פעולות על סדרות

פעולות בסיסיות:

- head(seq) – מחזירה את האיבר הראשון בסדרה. (תוצאה – איבר)
- tail(seq) – מחזירה את כל הסדרה למעט האיבר הראשון. (תוצאה – סידרה)
- front(seq) – מחזירה את כל הסדרה למעט האיבר האחרון. (תוצאה – סידרה)
- last(seq) – מחזירה את האיבר האחרון בסדרה. (תוצאה – איבר)
- seq1⁀seq2 – שרשור הסדרה seq2 לאחר seq1. (תוצאה – סדרה)
- seq(i) – גישה לאיבר ה-i בסדרה
- ניתן להתייחס לסדרה בתור מערך. גישה לאיבר במערך (בדומה לשורה הקודמת) נכתוב על ידי s(i). אם נתייחס למערך דו ממדי, נוכל לכתוב s(i)(j).

הפעלת פונקציה על איברי סדרה:

- נתונים:
  - תהי f פונקציה מעל איברים מסוג X.
  - תהי S סדרה של איברים מסוג X.
  - $S:seq[x];\ f:X \rightarrow Y$
- כדי להפעיל את f על כל איבר ב-S נכתוב: $S \cdot f$
- התוצאה היא סדרה של איברים מסוג Y.

5. סכמות (Schemas)

סכמה היא דרך שבעזרתה אנחנו מתארים מערכות. באמצעות סכמה אנחנו מתארים:

- המצבים הקיימים במערכת.
- תנאים מקדימים (preconditions) לפעולות השונות.
- השפעת הפעולות על מצב המערכת.

מערכת היא אוסף של סכמות המגדירות את המצבים, המצב ההתחלתי וההשפעות של כל פעולה.

תיאור התחלתי יכול להיות **מעודן** על מנת להתקרב יותר למימוש בקוד. נרחיב על כך בהמשך המסמך.

סימונים:

$a?$	קלט לפעולה
$a!$	פלט מפעולה
a	רכיב מצב לפני הפעולה
a'	רכיב מצב אחרי הפעולה
S	סכימת המצב לפני הפעולה
S'	סכימת המצב אחרי הפעולה
ΔS	שינוי במצב (לרוב $S \wedge S'$)
ΞS	אין שינוי במצב (לרוב $\left[S \wedge S' \mid \theta S = \theta S'\right]$)

נייצג סכמה בצורה הבאה:

$$S = \left[\text{declarations} \mid \text{predicate}\right]$$

המשמעות היא שרכיבי המערכת שבאיזור ה-declarations מספקים את ה-predicate.

מה המשמעות של S? S היא סכימה, והיא מתארת פעולה כלשהי. הפעולה ש-S מתארת מתבצעת על המשתנים המוגדרים באזור ה-declarations, ובסיום ביצוע הפעולה המשתנים יספקו את ה-predicate. חשוב לשים לב ש-S לא מתארת כיצד הפעולה תתבצע, אלא רק מה תהיה התוצאה.

6. מקורות

שקפי הרצאות מהטכניון, 2009, "מפרטים פורמלים למערכות מורכבות"

הספר "Formal Specification", מאת פרופ' שמואל כץ